УДК 004.056

В.Ф. Чекурін[1, 2]**, О.О. Будік**[1]
[1]Національний університет "Львівська політехніка",
кафедра захисту інформації;
[2]Інститут прикладних проблем механіки і математики
ім. Я.С. Підстригача НАН України

МОДЕЛЬ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВНЗ ТА ПІДХІД ДО ОЦІНЮВАННЯ ЇЇ РИЗИКІВ

Розглянуто типову структуру інформаційної системи вищого навчального закладу і навчальної інформаційної системи. Запропоновано підхід до оцінювання ризиків цих систем.

Typical structure of higher education information system and learning information system is considered. Approach to risk assessment for these systems is proposed.

Вступ. Сучасні технології навчання ґрунтуються на інтенсивному використанні інформаційних ресурсів та розподілених інформаційних систем (ІС) [1]. Безпека цих систем має важливе значення як для нормального функціонування навчального закладу, так і для забезпечення належної якості освіти. Порушення конфіденційності, цілісності та доступності інформації в навчальних ІС (НІС) може негативно впливати на навчальний процес, завдавати фінансових збитків, створювати незручності для студентів, викладачів та адміністративного персоналу. Навчальні ІС є складовими частинами інформаційних систем закладів освіти (ІСЗО). Інформаційні системи закладів освіти мають низку особливостей, що відрізняють їх від ІС інших установ, організацій, підприємств. Сьогодні ще остаточно не сформовані уявлення щодо оптимального складу таких систем, їх архітектури, функцій, які вони реалізують, а також не випрацювані підходи до забезпечення безпеки інформації в таких системах з урахуванням їх специфіки.

Метою цієї статті є опрацювання типової структури ІС та НІС ВНЗ, окреслення підходу до оцінювання ризиків інформаційній безпеці цих систем.

Організаційна структура ВНЗ та модель циркуляції інформації. Процеси вироблення, споживання та циркуляції інформації в закладі освіти істотно залежать від його організаційної структури. В Україні функціонують ВНЗ різних рівнів акредитації [2], які відрізняються організаційною структурою, інформаційними джерелами й потоками. Обмежимося тут розглядом структури ВНЗ типу "університет" [2] як організаційної структури, що поєднує інститути та кафедри. Для опрацювання структури ІСЗО розглядатимемо організаційну структуру університету як трирівневу (рис. 1).

Кожен рівень об'єднує адміністративно-господарську (АГЧ), навчальну (НЧ) та наукову (чи науково-дослідну, НДЧ) частини. Кожна частина має свої інформаційні ресурси (ІР), які формують ІР цього рівня. Інформаційні ресурси трьох рівнів формують ІР університету. Інформаційні ресурси різних рівнів і ВНЗ загалом є елементами як його організаційної структури, так і структури ІСЗО.

Інформаційні ресурси на будь-якому рівні ієрархії можуть обмінюватися інформацією з ІРЗО (інформаційні ресурси закладу освіти) інших рівнів та із зовнішніми ІР.

На рис. 2 зображено модель циркуляції інформації у ВНЗ. Відповідно до організаційної структури ВНЗ (рис. 1) інформаційні ресурси можна розглядати на трьох рівнях – ІР1 (рівня ВНЗ), ІР2 (інститутському рівні) та ІР3 (кафедральному рівні). На кожному з рівнів також є користувачі (К1, К2 і К3), які можуть бути продуцентами і споживачами інформації. Як показано на рис. 2, обмін інформацією може відбуватися всередині кожного рівня, між рівнями, а також із зовнішніми ресурсами.

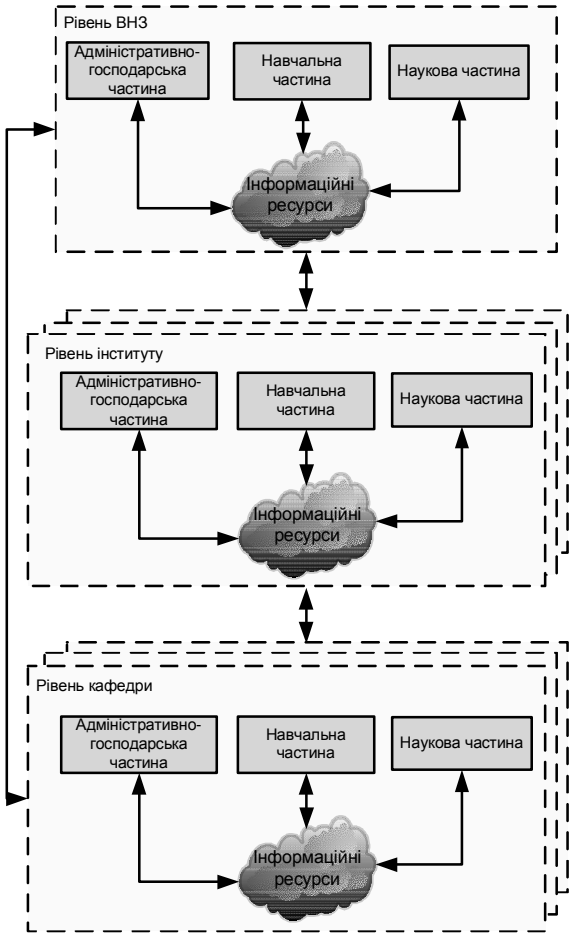

Рис. 1. Організаційна структура та інформаційні ресурси ВНЗ

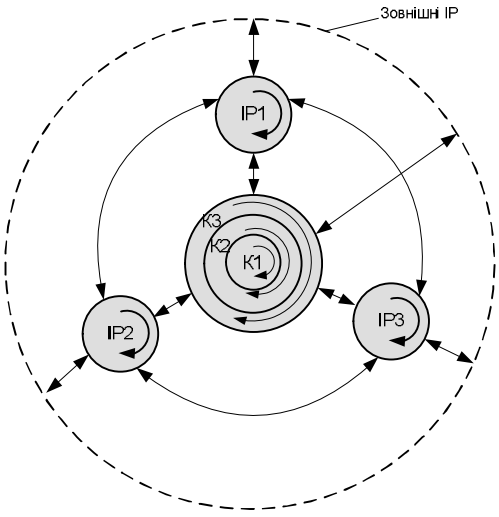

Рис. 2. Модель циркуляції інформації у ВНЗ

Структура інформаційних ресурсів ВНЗ. Інформаційні ресурси кожного рівня складаються із ІР АГЧ, НЧ та НДЧ, які, своєю чергою, можуть бути структуровані за організаційним та/чи функціонально-тематичним принципами. Зокрема, їх можна уявляти як ієрархічну деревоподібну структуру, у яку входить ІР структурних підрозділів, а також окремих користувачів (рис. 3).

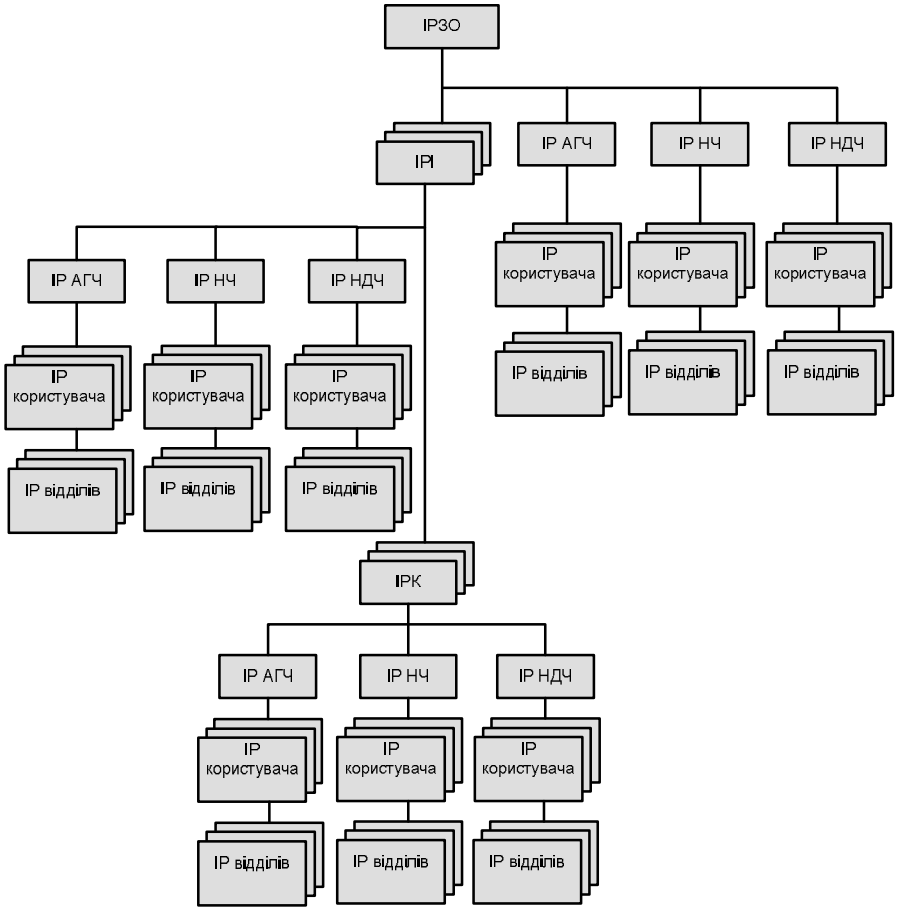

Рис. 3. Структура ІРЗО

Інформаційні ресурси на рівні ВНЗ об'єднують ІР АГЧ, ІР НЧ, ІР НДЧ та ІР інститутського рівня (ІРІ). Інформаційні ресурси на рівні інституту включать свої ІР АГЧ, ІР НЧ, ІР НДЧ та ІР кафедрального рівня (ІРК).

Інформаційна система ВНЗ. ІСЗО призначена для підтримки інформаційних ресурсів та потоків, надання користувачам інформаційно-обчислювального середовища та інших послуг, необхідних їм для виконання своїх функцій як викладача, науковця та адміністратора.

ІСЗО – організаційно-технічна система, в котрій реалізуються інформаційні технології, і передбачається використання апаратного і програмного забезпечення, необхідного для реалізації процесів збирання, обробки, накопичення, зберігання, пошуку і поширення інформації. Основою інформаційної системи вищого навчального закладу є територіально розподілені комп'ютерні системи (обчислювальні мережі), елементи яких розміщені в окремих будівлях, на різних поверхах цих будівель і пов'язані між собою транспортним середовищем (скручена пара, оптоволоконні канали, радіоканали тощо). Основу апаратних (технічних) засобів таких систем становлять персональні обчислювальні машини, периферійні та інші допоміжні пристрої, засоби зв'язку. Склад програмних засобів визначається можливостями апаратури і характером вирішуваних завдань в конкретній інформаційній системі.

Можна виділити такі елементи ІСЗО:

- апаратне забезпечення;
- програмне забезпечення;
- інформаційні ресурси;
- автоматизовані робочі місця користувачів (АРМ);
- власне користувачі.

Зважаючи на це, можна побудувати модель ІСЗО (рис. 4).

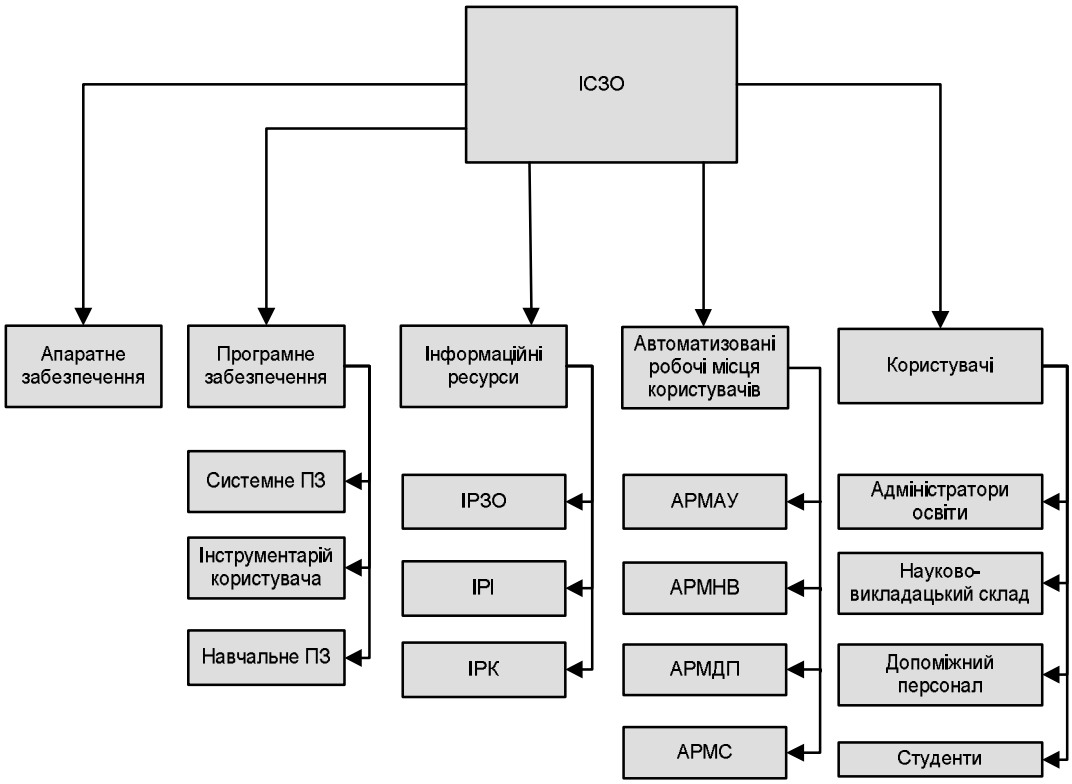

Рис. 4. Модель ІСЗО

Апаратне забезпечення – це канали і засоби зв'язку, вузли комутації, сервери тощо. Програмне забезпечення ІСЗО об'єднує системне програмне забезпечення, необхідне для підтримки функціонування самої системи, інструментарій користувача та навчальне програмне забезпечення. Структуру інформаційних ресурсів наведено у параграфі 2. Автоматизовані робочі місця відповідно до чотирьох типів користувачів можна поділити на АРМ адміністративно-управлінського персоналу (АРМАУ), АРМ навчально-викладацького складу (АРМНВ), АРМ допоміжного персоналу (АРМДП) та АРМ студентів (АРМС).

Навчальні інформаційні ресурси. До навчальних інформаційних ресурсів (НІР) належать матеріали в електронному вигляді, які можуть використовувати користувачі (викладачі та студенти) у навчальному процесі. Зокрема, до них зараховуватимемо підручники, монографії, конспекти лекцій, навчальні презентації, навчально-методичні матеріали, інструкції до виконання лабораторних робіт, завдання до самостійних, розрахункових, курсових, дипломних робіт (проектів), тестові завдання тощо. Крім того, до цих ресурсів зараховуватимемо інформацію щодо організації навчального процесу – розклади занять, контрольних заходів, екзаменів, консультацій, списки заборгованостей тощо.

Відповідно до продуцентів та споживачів цих ресурсів їх зараховують до кафедрального, інститутського та університетського рівнів. Кафедральний рівень об'єднує навчальні інформаційні ресурси, які створювані та використовувані користувачами, організаційно підпорядкованими цій кафедрі (студенти, викладачі та адміністративний персонал кафедри). Сюди входять навчально-методичні матеріали кафедри (НММК), навчальні матеріали кафедри (НМК) та матеріали для перевірки знань (МПЗК). Інститутський рівень об'єднує інформаційні ресурси, спільні для усіх користувачів, які організаційно підпорядковані цьому інститутові. Зокрема, сюди входять НІР кафедрального рівня (НІРК), а також навчально-методичні матеріали інституту (НММІ), навчальні матеріали інституту (НМІ) та матеріали для перевірки знань (МПЗІ), розроблені на рівні інституту. До інформаційних ресурсів університетського рівня належать загальні інформаційні ресурси – бібліотека студентська (СБ) та наукова (НБ), НІР інститутського рівня (НІРІ), навчально-методичні матеріали (НММУ), навчальні матеріали (НМУ) та матеріали для перевірки знань (МПЗУ), розроблені на найвищому рівні – рівні університету. Окремо слід виділити зовнішні навчальні інформаційні ресурси (ЗНІР).

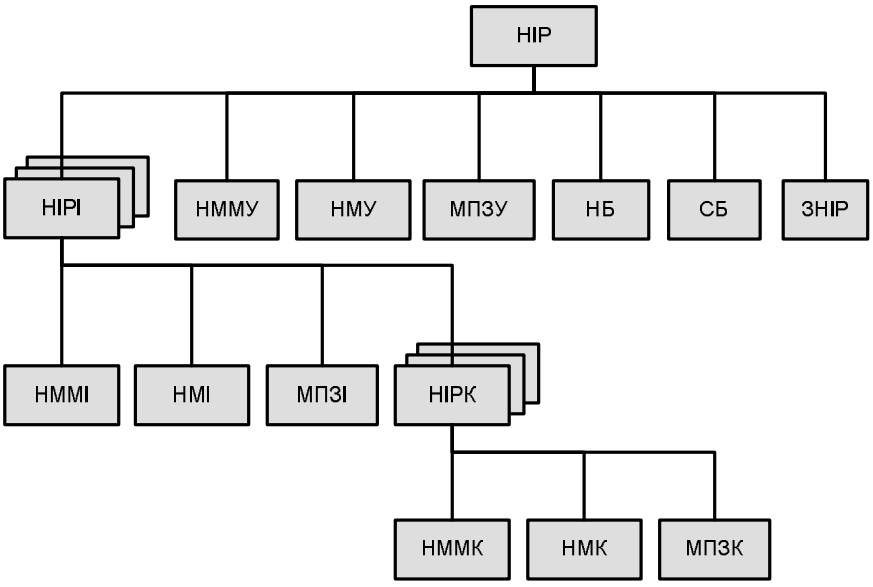

Рис. 5. Структура НІР

Структура навчальної інформаційної системи ВНЗ. Навчальна інформаційна система є складовою ІСЗО і призначена для надання доступу користувачам до навчальних інформаційних ресурсів, а також контролю знань студентів і аспірантів. Складовими НІС є навчальні інформаційні ресурси, інструментарій користувачів, інтерфейси користувачів, підсистема контролю успішності.

Структуру навчальних інформаційних ресурсів розглянуто вище. В інструментарій користувачів входить інструментарій викладачів та інструментарій студентів. До інструментарію користувачів належать офісні програмні пакети, спеціалізовані програмні продукти, інші прикладні програми тощо. Інтерфейси користувачів об'єднують інтерфейс викладача та інтерфейс студента. Інтерфейс викладача дає змогу розміщувати навчальні матеріали, матеріали для контролю знань, отримувати доступ до результатів успішності тощо. Інтерфейс студента дає змогу користуватися навчальними матеріалами, проходити контроль знань тощо. Підсистема контролю успішності забезпечує ведення електронних версій залікових відомостей і журналів відвідування.

Використання CVSS для оцінки вразливостей НІС та ІСЗО. Загалом методологія CVSS (Common Vulnerability Scoring System) призначена для ранжування та оцінювання вразливостей інформаційних систем. У нашій роботі пропонуємо використати CVSS для оцінки ризиків інформаційній безпеці ІСЗО та НІС ВНЗ.

Загальна система оцінки вразливостей (CVSS) [3] – це відкрита схема, яка дає змогу обмінюватися інформацією про вразливості в інформаційних системах. CVSS складається з трьох метрик: базова метрика, часова метрика, контекстна метрика. Кожна метрика являє собою число (оцінку) в інтервалі від 0 до 10 і вектор – короткий текстовий опис зі значеннями, які використовуються для виведення оцінки. Базова метрика відображає основні характеристики вразливості. Часова метрика відповідає таким характеристикам вразливості, котрі змінюються з часом, а контекстна метрика – характеристикам, які унікальні для середовища користувача. CVSS є зрозумілим, прозорим і загальноприйнятим способом оцінки вразливостей для керівників, виробників програмного забезпечення і засобів підтримання інформаційної безпеки, дослідників тощо.

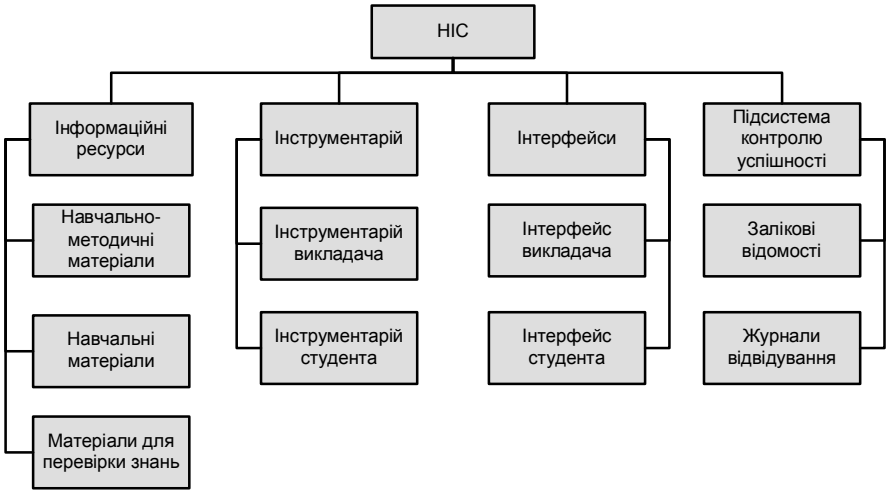

Рис. 6. Структура НІС ВНЗ

Група базових метрик відображає характеристики вразливості, котрі не змінюються з часом і не залежать від контексту. Метрики AV (Access Vector, Вектор доступу), AC (Access Complexity, Складність доступу) і AU (Authentication, Аутентифікація) оцінюють, як отримати доступ до вразливості і чи потрібні для експлуатації вразливості додаткові умови. **Три метрики впливу** – CI (Confidentiality Impact, Вплив на конфіденційність), II (Integrity Impact, Вплив на цілісність) і AI (Availability Impact, Вплив на доступність) – описують можливий прямий вплив на систему у випадку експлуатації вразливості.

Загроза, котру зумовлює вразливість, може змінюватися з часом. Є три фактори, котрі змінюються з часом і враховуються в CVSS: підтвердження технічних деталей вразливості, статус виправлення вразливості, доступність коду експлуатації чи технології експлуатації. До **часових метрик** належать: E (Exploitability, Можливість використання), RL (Remediation Level, Рівень виправлення), RC (Report Confidence, Ступінь достовірності).

Різні середовища можуть мати величезний вплив на ризик, котрий викликає наявність вразливості, для організації і зацікавлених осіб. **Група контекстних метрик** CVSS відображає характеристики вразливості, котрі тісно пов’язані із середовищем користувача. До контекстних метрик належать: CDP (Collateral Damage Potential, Імовірність завдання побічного збитку), TD (Target Distribution, Густина цілей), SR (Security Requirements, Вимоги до безпеки). Метрика “Вимоги до безпеки” містить три метрики: CR (Confidentiality Requirement, Вимоги до

конфіденційності), IR (Integrity Requirement, Вимоги до цілісності), AR (Availability Requirement, Вимоги до доступності).

Як ми вже зазначали вище, інформаційну систему закладу освіти та навчальну інформаційну систему ВНЗ можна розглядати на трьох рівнях. На всіх цих рівнях є свої інформаційні ресурси, що потребують захисту. Атаки на ці ІР можуть здійснюватися за наявності вразливостей у ІСЗО та НІС.

На рис. 7 наведено дерево напрямлених графів. Вершинами графів є значення метрик CVSS. Базові метрики формують імовірність атаки з використанням цієї вразливості. Чим меншою є складність експлуатації вразливості, тим більша імовірність, що зловмисник здійснить атаку за допомогою цієї вразливості (ЧА, частота атаки). За допомогою часових метрик отримуємо уточнювальний коефіцієнт (УК), який разом із ЧА формує уточнену оцінку УЧА (уточнена оцінка імовірності атаки). Контекстні метрики враховують важливість вразливості і небезпеку її реалізації для конкретного середовища (вплив).

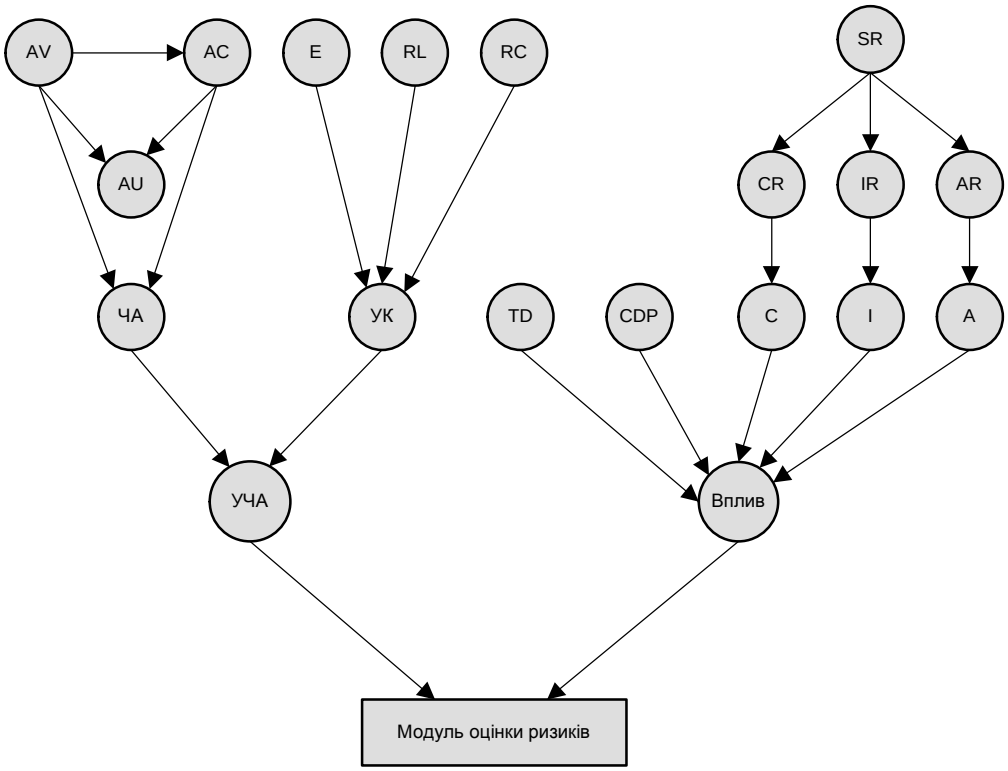

Рис. 7. Оцінка ризиків з використанням метрик CVSS

На підставі [4] у найпростішій формі ризик r для цієї загрози розраховується як:

$$r = Cp, \tag{1}$$

де C є потенційною втратою вартості ресурсу (що можна інтерпретувати як вплив від реалізації вразливості), а p – імовірність атаки на цей ресурс (в нашому випадку ЧА чи УЧА).

Для i-ї вразливості v_i загальний ризик R_i, який існує для мережі з N ресурсів, можна визначити за формулою:

$$R_i = \sum_{j=1}^{N} c_j \sum_{k=1}^{k_j} t_{kj}(v_i)\, p(t_{kj}(v_i)), \tag{2}$$

де t_{kj} – потенційна втрата вартості j-го ресурсу, спричинена k-ю загрозою з використанням i-ї вразливості v_i.

Для i-ї вразливості v_i загальний ризик R_i, який існує для мережі з N ресурсів, можна визначити за формулою:

$$R_i = \sum_{j=1}^{N} c_j \sum_{k=1}^{k_j} t_{kj}(v_i)\, p(t_{kj}(v_i)), \qquad (3)$$

де t_{kj} – потенційна втрата вартості j-го ресурсу, спричинена k-ю загрозою з використанням i-ї вразливості v_i, m_{ikj} – зменшення імовірності експлуатації вразливості v_i для загрози t_{kj} завдяки засобам захисту.

На підставі формул (1–3) може бути реалізований модуль оцінки ризиків (рис. 7). Отже, від оцінки окремих вразливостей ми можемо перейти до оцінки ризиків як окремих елементів ІСЗО та НІС, так і цих систем загалом.

Висновки. У цій роботі запропоновано типову структуру інформаційної системи закладу освіти та її підсистеми – навчальної інформаційної системи. Одержані моделі дають змогу на концептуальному рівні розглядати ці системи з метою аналізу можливих вразливих місць та оцінювання ризиків інформаційній безпеці вищого навчального закладу.

Також розроблено підхід для оцінювання цих ризиків, який ґрунтується на використанні методології Common Vulnerability Scoring System (CVSS). Застосування метрик CVSS, на відміну від інших складних кількісних підходів, дає змогу значно спростити процес оцінки ризиків. Запропонований підхід зручний і зрозумілий у застосуванні, оскільки використовує стандартизовані метрики та прості математичні обчислення.

1. Сєркова Л.Е. Інформаційна технологія моніторингу організації учбового процесу вищого навчального закладу: дис. канд. техн. наук: 05.13.06 / Черкаський держ. технологічний ун-т. – Черкаси, 2006. 2. Закон України "Про вищу освіту". 3. Peter Mell, Keren Scarfone, Sasha Romanovsky. A Complete Guide to the Common Vulnerability Scoring System. Version 2.0. FIRST, 2007. 4. Maxwell Dondo. A Fuzzy Risk Calculation Approach for a Network Vulnerability Ranking System. Defence R&D Canada – Ottawa, 2007.